DISCUSSION PAPER

ON IMPLICATIONS OF THE PROPOSED GENERAL REGULATION ON DATA PROTECTION FOR HEALTH AND eHEALTH

Proposed by the eHealth Governance Initiative

Date: October 22nd 2012

Preamble

During their spring meeting, the eHealth Network requested that the eHealth Governance Initiative (eHGI) present a Discussion Paper on the proposed Data Protection Regulation, drawing on the responses to national consultations on the draft legislation.

This Discussion Paper has been produced by the eHGI – member countries, industry and NGOs – and provides an overview of common issues of concern. It is therefore not intended to reflect the positions of individual Member States or to interfere with the national review process of the Regulation.

The Discussion Paper draws upon a survey which was launched by the eHGI during the summer amongst its members. In what concerns cross border eHealth, the paper also draws upon the Recommendations of epSOS and the WP29 Opinion on epSOS issued in spring 2012. The consolidation of information and input from 19 Member States, health professionals and industry were discussed during a workshop on September 4th 2012.

Data protection, a critical matter for eHealth

When an eHealth solution is the primary vehicle for supporting the delivery of care, both across borders and within Member States, the number of data protection issues is high. Data is not only shared for the provision of immediate care, but could be used again ("secondary use") for service planning, reimbursement, auditing and research.

There are three over-riding principles, which are in conflict in some situations:

- The proposal for a Data Protection Regulation aims to ensure that all individuals in the EU enjoy a ***consistent level of data protection and rights,*** which will include access to personal data and the deletion or suppression of sensitive information;
- There must be a ***right balance*** between benefits and costs and between medical needs and the protection of privacy, as well as between the interests of the individual patient [data subject] and the interests of the public health of a nation or region.
- The safe transfer of data within and between Member States needs to be managed with appropriate levels of data protection. ***The legislation should be seen as a vehicle to facilitate the safe transfer of data for eHealth***, and not as a tool to hinder the sharing of information, be it within a Member State's healthcare system or across borders.

It is also noted that the main issues addressed in this paper do not represent an exhaustive list; rather they present an indicative account of the issues identified by the consulted parties as concerning eHealth.

1. Definitions (Article 4)

The definitions and concepts address a very broad audience and are common to both the Regulation and the EU Directive for the processing of personal data by competent Authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or for the execution of criminal penalties. The two instruments are subject to parallel consultation, both in terms of process and participants.

In particular, *the definition of personal data may vary according to the scope, interests or applicable standards; likewise, this definition is crucial when interpreting the provisions of the Regulation as well as the limitations and exemptions*.

2. Legal basis for processing health data – Consent

Generally, sensitive data must not be processed without explicit consent from the data subject; however, consent is not always required, nor is it the primary legal grounds for processing health related data. Ethical, regulatory and human rights instruments are also of relevance. Within the context of necessary or immediate healthcare, the standard practice is for treatment to be provided on the basis of implied consent. It therefore follows that information is only shared in the same context on a "need to share" basis and within a defined healthcare team (the members of which will change depending on the care provided). Data protection and privacy legislation, professional and contractual regulations and an audit trail are the main elements that deter or punish the inappropriate sharing or disclosure of information.

Beyond team-based healthcare, there is a wide variety of potential "secondary" use of data which is open to healthcare professionals outside the team: social care providers, insurers, technical staff, researchers and others. Both access to and the use of patient information must be covered by "appropriate" levels of consent. In terms of healthcare data, "appropriate" means a level of consent that is fully informed in terms of the purpose for which the data will be seen, shared or processed, the security of the system holding it, and ensuring that means exist to track the identity, role and authority of all individuals who access it.

Consent remains a top priority with significant cultural variation across the EU in terms of its construction of purpose and extent, and continues to create issues between countries in cross border transfers. *Derogations for sensitive data in the Regulation include derogations for procedures for settling claims within health insurance systems; for historical, statistical and scientific research purposes (usually with anonymisation of data), and in exceptional situations where public or personal interests take precedence over privacy concerns, such as child protection.*

It is noted that the Opinion of the Art 29 Working Party for the epSOS pilot cross border services is that neither Art 8(3) of the Directive 95/46, which creates an exception to consent for medical treatment, nor Art 8(4) on public interest could be invoked as these would require the full purposes for which cross border access may be granted to be made explicit. Therefore

in epSOS, explicit consent and Art 8(2) (c) – vital interests – are used as the legal basis for the transfer of data. As explicit consent cannot be given for an anticipated but unknown event, consent is provided in two steps: firstly for data collection/adaptation for epSOS in the country of residence and secondly for data transfer and processing for a specific epSOS incident in the country of treatment.

Practical and proportionate procedures for obtaining and recording consent are needed and must fit in with current processes of care. Systems must also address the fact that sometimes medical emergencies will require that information is shared without consent when the patient is incapacitated. A full audit must be in place for any occasion in which data is shared without consent. *Interpretation of these exceptions is subject to varying national concepts of incapacity as in the case when treating children or for situations in which disclosure is required by law, such as child protection or when controlling outbreaks of infectious diseases.*

3. Specific challenges for access to data in healthcare settings

It is important to differentiate between the purpose and needs for data collection, sharing and processing in healthcare settings: the quality and safety of clinical care depends on the availability of personal health ***data***, which is collected locally in care records and may be stored, shared or processed in regional, national or cross border settings for providing care, under specific conditions and safeguards.

Public health services rely upon ***information*** which is often extracted from care records to be re-used; health and social insurance systems also need this kind of information for the purposes of planning, reimbursement, auditing and statistics. Health information may therefore be shared across public authorities, under specific conditions and safeguards. As a rule, information of this kind can be and should be anonymised. Any data processor accessing patient-identifiable information for secondary use should be able to justify why this is necessary, and demonstrate that consideration has been given to aggregating and/or anonymising the data.

Advancing medicine through public health and scientific research creates ***knowledge*** which may be based on health data as its primary source; however sources of this kind can again be anonymised.

4. The right to be forgotten

In healthcare, there is a need to retain data inter alia in the interest of the patient and to provide evidence of the accountability of the doctor and overall legal certainty. Therefore, it seems important that healthcare data should be stored with the appropriate security standards in order to allow the medical treatments and decisions made by any European health professional to be proved to the highest degree of legal certainty and accountability.

Whereas the Regulation makes specific provisions and exceptions for public health, the scope as defined in recital 123 is not sufficient to address the variability of purposes in the healthcare settings. For example, Article 17.3 (b) introduces an exception to the retention of the personal data "for reasons of public interest in the area of public health in accordance with article 81 (Processing of personal data concerning health)"; however, the reference made to the public interest in both cases is neither precise enough nor sufficient**.**

From a clinical, financial and research perspective, there are implications of deleting data from electronic records. Some elements of information from the deleted record will most likely have been extracted at the time of creation and throughout the use of the shared record. Each of these derived elements of information represents distributed traces that take a variety of forms given the clinical activities performed. Thus they are difficult and sometimes impossible to track electronically[1].

Most importantly, incomplete medical records may harm patient care in circumstances where the treating physician has an incomplete record. Solutions to this dilemma include ensuring that a trace (or "flag") is left whenever information is deleted/suppressed, indicating that some information is hidden and that patients are fully advised about the possible consequences of removing access to potentially important information.

5. Implementation Challenges

5.1. Delegated Acts

The number and scope of delegated and implementing acts undermine the legal certainty of the Regulation in terms of its content and the time-line for its adoption, and introduce the risk of overly prescriptive interventions (e.g. prescriptive standards or technology). In some cases, the provisions for delegated acts also entail implementation risks. For example, the European Commission may adopt a delegated act to specify the criteria for categories of recipients of personal data; however, the number and categories of recipients accessing the data for one episode of care in a hospital is too large and too complex to be prescribed.

5.2. Time until enforcement

The time suggested to apply the Regulation following its publication may not be realistic for healthcare due to major legal, organisational and technical challenges. Member States need to harmonize and consolidate legislation about health documentation with health data, for example, as a duty to maintain records. The implementation of consent including consent for children entails organisational challenges and financial implications. Implementing citizens' access to personal data/information and their right to obtain a copy of data in an understandable format would require legal and technical interventions into the national [legacy] systems.

[1] When it is created and shared, the record to be subsequently deleted has to be traced (without the risk of being tampered with) into a number of logs managed by the systems it traverses, e.g. care delivered resulted in quotations in various forms as well as clinical decisions made on the basis of the subsequently deleted record; the patient may have made copies in the cloud on the internet and forgotten about these copies.

6. Proposals and next steps

1. *The eHGI submits that*
    - *Definitions should be appropriately reviewed to ensure alignment with concepts, current usage and the needs of the diverse eHealth stakeholder community.*
        - *In particularly challenging areas, especially where there is rapid technological evolution – such as anonymisation and pseudonymisation – definitions should be set out clearly in the legislation, and the processing of this data should not be subject to any further requirements of the legislation other than compliance with the applicable standards.*
    - *Certainty should be improved in areas such as derogations on the grounds of public interest and – in what concerns the processing of health data – scope which extends beyond public health.*
    - *It is desirable to clarify the proposed exceptions as regards the "right to be forgotten" and to extend the scope so that the exceptions apply to "healthcare data". Likewise, the financial impact and technical feasibility of certain provisions need to be further assessed.*

2. *On the basis of the above considerations, it is evident that the article by article discussion in DAPIX is not likely to address the complexity in eHealth. Promoting the issues appropriately under subject headings and in an approach which is coordinated by the Member States under the eHealth Network could prove more useful.*